

HQ USEUCOM Security Assistance Office Automation Guide





HEADQUARTERS
UNITED STATES EUROPEAN COMMAND
UNIT 30400 BOX 1000
APO AE 09128

Logistics and Security Assistance Directorate

The world of automation continues to improve our work environment daily. The introduction of new technologies presents endless challenges, as we become more dependent upon office automation.

This guide provides the ground rules for information assurance, which lays down the minimum requirement for protecting the office environment from harmful, external intrusion. Additionally, it puts the key small office automation tools together in one desktop reference. It gives you the pros and cons of various automation systems and services, which should help you to set up and maintain your office automation assets. You are encouraged to seek other sources of information to further develop your office automation solution. Use this guide to design your office automation plan, but keep your plan up to date and it will serve you and those that follow you well.

We hope this office automation guide will help you manage your office automation systems in support of your security assistance mission. We welcome your suggestions for its improvements.



LARRY LUST
Major General, USA
Director of Logistics and
Security Assistance

TABLE OF CONTENTS

Part I:	General Information
Part II:	Information Assurance
Part III:	Hardware
Part IV:	Software
Part V:	Networking
Part VI:	Communications and Internet Access
Part VII:	The “Primary Road Map”
Part VIII:	Reference Library
Appendix 1:	ADP Plan Overview
Appendix 2:	ADP Plan Template
Appendix 3:	LAN Cable Specifications
Appendix 4:	Sample Computer Users Agreement
Appendix 5:	Computer Security Pamphlet

PART I: GENERAL AND ADMINISTRATIVE INFORMATION

This guide will provide information for you to consider in developing your office automation plans. The majority of the information is intended for those who are not automation “experts.” Most of the information and guidance you will find in this guide is based on successes – and failures - we’ve seen recently in small office automation.

Information and considerations in this guide are intended for the automation beginner and for small to mid-size USEUCOM SAOs; about 3-12 people. We’ll cover the topics and try to tie them together into a package that makes sense for most USEUCOM Security Assistance Offices (SAO). We realize that each office is different, that there are outside considerations (embassy requirements), and that there are differing levels of expertise within each SAO. This guide is not intended to be the “school solution”, but a road map, with some detours, to help you get to the level of office automation you feel you need to meet your Security Assistance mission requirements.

Mandatory “Stuff”

USEUCOM Standards: There is only one mandatory requirement that we are going to impose on you. Any software you use must be compatible with the USEUCOM standard and Security Assistance specific software. The reason for this is obvious: Uniformity throughout the command. We want you to be able to read our “stuff” and we want to be able to read yours. You don’t want to go through a massive conversion routine when we send you something electronically, and neither do we. When the USEUCOM Standard changes we’ll let you know. Concurrent with any change notification will be authorization to purchase new software. See Part IV Software, for current software standards.

The lowest common denominator: There is frequently a self appointed computer expert in many SAOs who knows – or seems to know – more about automation than anyone else in the office. This can be both a blessing and a major cause of problems; especially after the person PCSs and things start to break. The KISS (Keep It Simple Stupid) principle is absolutely what you want to keep uppermost in your mind when creating or upgrading any office automation. Design your office to be simple and efficient. The fewer the bells and whistles, the fewer the problems. People who come into the office after your “expert” departs at the end of their three year tour may not have any idea how to maintain the system you have in place. Their knowledge of computers may be limited to knowing where the on-off button is.

Maintain documentation or schematic diagrams: Make sure the expert writes everything he/she does down on a piece of paper! If your system goes down this will make it much easier to track down and fix problems. If you’re hooking everything into a network, this is essential for later repairs or upgrades. How many times have you tried to track down and repair, or re-install, wiring for your home stereo system and spent hours trying to figure out why the thing doesn’t work! Same thing – only worse - for a local area network in a 10 person ODC. If someone from the outside (like us) comes in to help you “fix” your system or network, a simple schematic and some documentation will help tremendously.

Support from the headquarters: We will provide technical assistance and support for USEUCOM standard software, and for Security Assistance specific software (e.g. SAN Web, TMS, and SAARMS). We don't have the time, money, or manpower to be expert in non-standard systems or software. If you deviate from the USEUCOM standard then you do so at your own peril. Make sure you've got local "tech support" built into your acquisition planning.

PART II: INFORMATION ASSURANCE

Purpose

As a computer user, your actions can greatly increase or decrease the integrity, availability, and confidentiality of information concerning national defense. Protecting that information is called “information assurance.” This guide will help you understand and enforce information assurance by showing you how to recognize and avoid the hazards awaiting you once you enter the “information highway.”

Your Computer as a Gateway to Information

Your computer has access either through your local area network (LAN) or your Internet Service Provider (ISP) to the Internet. As a user of a computer in USEUCOM, you play a key role in ensuring the availability, confidentiality, and integrity of our data. Pay attention to what follows, and you will not be the weakest link. If you can get out, a hacker can get in. A basic premise of networked computing is that if you have access to the Internet through your computer, hackers have access to you. Remember that the information highway is a two-way street.

How to Treat Your Computer

- Your computer is an important part of the toolkit you need to do your job. Treat your computer with care. One of the most important things you can do is keep the temperature and humidity correct in your office. Heat is your computer’s worst environmental enemy. Exposing your computer to heat will shorten its life span and put your data at risk.
- Do not eat or drink near your computer. Spilling soft drinks, coffee, or other liquids on your computer can damage it and destroy your files.
- Keep your system clean and free of dust.
- Do not disconnect your computer from its network. The small network connections are very fragile and very expensive.
- Turn your computer off at the end of the day. If your computer is turned off, it cannot be hacked.

Personal Use of Your Government Computer

We have detailed rules for appropriate and inappropriate use of Government computers. We also have rules governing how you may use your Government computer for personal use. The U.S. Government provides you with a computer to do your assigned duties. The rules are simple and clear. Government computers may be used only by Government employees for the following:

- Official business related to your official duties.
- Authorized personal use includes brief access and searches for information on the Internet and sending short e-mail messages.
- SAO Chiefs and supervisors must make every effort to ensure that personal use of Government computers:

- (1) Does not adversely affect the performance of official duties.

(2) Is limited to reasonable duration and frequency and, when possible, done during off-duty hours.

(3) Serves a legitimate public interest, such as keeping employees at their desks, furthering the education and self improvement of employees, improving employee morale and welfare, or job-searching in response to downsizing.

(4) Personal use of Government computers must not overburden the communications system.

(5) Personal use of Government computers must not reflect adversely on DoD or DoD components.

(6) Misuse of Government computers includes hacking or using hacker tools, visiting hacker websites, deliberately installing viruses on DoD computers, trying to mask or hide your identity, attempting to bypass security policy, using Internet telephony, streaming audio/video (such as receiving hourly stock updates), and using Hotmail, Rocketmail, and Yahoosail for other than morale, welfare, and recreation.

- Penalties for misuse of Government computers range from courts-martial to nonjudicial and administrative actions, such as letters of reprimand.

The Importance of Passwords

Your password is the key that gets you onto the information highway. Maintaining the security of your password is therefore one the most important security precautions you must take as a user.

You should not write down your password, nor should you ever share your password with anyone. If your password is compromised, a computer intruder can access all data to which you have access.

Passwords should be at least eight digits long, include at least two numbers, and not form a word or acronym. Passwords should be changed, at a minimum, every 6 months on a nonsecure system, and every 3 months on a secure system.

Passwords that do not conform to the standards above are very vulnerable to password-cracking programs continually used by hackers. Once hackers gain access to your computer, you have given them full reign of the DoD network. Password protection is therefore essential.

Detecting and Preventing Viruses

The best course of action is to prevent viruses from infecting your computer. Here are some things you can do:

(1) Make sure your system boots from the hard drive first.

(2) Use the current, DoD-authorized version of anti-virus software. You should update your anti-virus software every 2 weeks at a minimum; more frequently is even better. Set your computer to perform a live update of your anti-virus software at least twice a month. Remember that the developers who create anti-virus software are always slightly behind those who are creating new viruses. The more you update your anti-virus software, the better.

Installing anti-virus software is easy and free. You can also download the anti-virus software paid for by the DoD and install it on your computer at home. Ask your systems administrator or your Information System Security Officer (ISSO) about this, or use the DoD Computer Emergency Response Team, (DoD-CERT), webpage to get a free copy of the software (<http://www.assist.mil>). The Symantec AntiVirus Research Center webpage (<http://www.symantec.com/avcenter/index.html>) is another excellent source of information.

Even when taking the best precautions, viruses can still occur. They are not always immediately identifiable. Here are some things that may indicate the presence of a virus:

- (1) Abnormal activity or unexpected activity, such as abnormal displays or banners.
- (2) An unusually slow processing speed.
- (3) Unusual activity, error messages, changes in file sizes, and loss of programs or data.

If you find a virus, contact your security manager immediately. Prompt reporting of viruses can lessen their effect by giving security officers time to warn coworkers, who can then check their computers for the virus. If you have a new virus, chances are good that others in your organization will have the same virus. If your system is infected, first make sure you have the most current version of anti-virus software, then disinfect all files. Update your anti-virus software frequently, scan all diskettes, and be sure not to open suspicious e-mail attachments.

Chain-Mail, Virus Hoaxes, and Other Computer Hoaxes

Virus hoaxes are not real viruses and can be harder to get rid of than a real virus. Virus hoaxes and other e-mail hoaxes take up space on e-mail servers, use up network bandwidth, and waste time. Virus hoaxes are more common (and sometimes more time-consuming) than actual viruses. They usually take the form of e-mail warnings sent to large numbers of people to warn them about nonexistent viruses. Before you forward warnings such as these, read the Hoaxes & Scams page on the DoD-CERT webpage, the USEUCOM virus webpage (<http://www.eucom.mil/virusfaq.htm>), or the Symantec AntiVirus Research Center webpage (<http://www.symantec.com/avcenter/index.html>).

If you receive a message that appears to be chain-mail or a hoax, do not forward the message. The instructions usually include phrases like "pass this to everyone you know." Instead, inform your Regional Security Officer (RSO) or ISSO of the subject and source of the message, then delete it.

Travelling with a Laptop

When travelling with a government owned laptop do not use it to conduct office-related work in public areas. Think OPSEC! In addition to operational security, always maintain good physical security habits and keep your laptop within reach. Loss of automation equipment put key information in the wrong hands and poses a possible threat.

Reporting Policy

Users are often the first in the command to recognize a new virus. Reporting viruses to your RSO, ISSO or Information System Security Manager (ISSM) as soon as you detect a virus will greatly increase the chances of catching and stopping the virus from spreading. Other users can be warned and, subsequently, update their anti-virus software and scan their system for any new viruses. Early reporting of viruses also gets the word to computer users not to open e-mail attachments that contain the virus; warnings such as these are the best way to limit the spread of viruses that are transmitted in attachments.

Users are also among the first to notice intrusions by hackers. Some indications of a possible intrusion are seeing a web-browser open on your screen without your having opened it, noticing your CD-ROM drive trying to read a compact disk (CD) without your prompting it, or finding that your files are mysteriously being deleted or moved. If any of these things are happening, you may be the victim of a hacker and must report the incident to your RSO, ISSO or ISSM immediately.

Monitoring

Your use of a Government computer constitutes consent to monitoring. When you click "OK" on the network warning banner (which is required), which opens when you start your computer, you are giving your consent to having your computer monitored. Your Government computer is provided to you for authorized use only. Government computers are monitored to ensure that use is authorized and that users follow security procedures. Monitoring is also done to see if hackers have gained access to computers.

Conclusion

As a USEUCOM computer user, you play a key role in protecting the integrity, availability, and confidentiality of USEUCOM data. To recap:

- √ Guard your password.
- √ Follow the rules on personal use of your computer.
- √ Never forward chain-mail or computer hoaxes.
- √ Keep your anti-virus software up-to-date.
- √ Report viruses and all other network-security incidents to your appropriate security manager.

Taking the steps listed above will help you ensure that your computer and all networks to which your computer is connected are safe. In doing so, you will not only be protecting yourself, you will be protecting the entire command.

PART III: HARDWARE

Any hardware you use must be accredited. You, as the user, must maintain property accountability. You cannot bring your own hardware to work. Any hardware your office buys must meet DoD (DoD 5200.40) accreditation standards and be accounted for properly.



Personal Computers (PCs) This one is easy. Buy the best you can – within reason - and budget limitations. As this guide is being written a reasonable or normal standard for any PC is: Pentium II, 450 MHz, 6 Gigabyte hard drive, with 128 Megabyte RAM, 32 X CD, and other “stuff”. By the time you read this guide, the bar will have been raised and you’ll probably be able to buy a more capable computer for less money. The key thing is buy what the office needs and can afford.



A few offices have learned the hard way that the cheapest price is not the best buy. Buy your computer from a reputable company that can provide service locally if your computer needs maintenance. Some brands to consider are Compaq, Dell, Gateway 2000, Hewlett Packard, and Micron. Make sure that follow-on support is available, or not a problem. Gateway and Dell are good computers, but since they’re strictly mail order you need to ensure mailing a broken computer back for repairs won’t cripple your mission. Compaq and Hewlett Packard might have local maintenance capabilities.

Portable Computers (Laptops) The SA business requires that we travel frequently. Laptop computers keep us in touch with the office and enable us to do a lot of work while on the road. For the most part we tend to use laptops that enable us to send and receive e-mail, do word processing, and show a presentation. When you buy a laptop keep these things in mind. Our business requirements tend to run towards “plain vanilla.” Since laptops are more expensive than comparable desktop PCs, you can keep the cost down by buying a laptop that meets basic requirements without a lot of unneeded “bells and whistles”. You won’t need a big hard drive (but make sure you get enough space to install all needed programs), but get a fast processor (i.e., 350 +), sufficient RAM (64 +), and as fast a modem as possible (56K).



As a rule of thumb we recommend one laptop for every 3-5 action officers who are required to travel frequently, and need word processing, presentation, Internet, and e-mail capabilities while they are traveling. Make sure you can justify additional laptops in your ADP plan if your office needs dictate more laptops than the rule of thumb. Remember that you don’t need a laptop for every person in the office. You can also use the laptop as a PC in the office when not on the road, with the added expense of a docking station.

New light-weight laptops are less powerful, but a great option for frequent travelers (weight is ½ to 2/3 of a standard laptop).

Printers

- Laser Printers – designed for high use black and white printing (fast and cost effective).
- Ink Jet Printers – inexpensive to purchase, but printing is more expensive and slower.
- Color Printer – you’ve got two options: high cost, high speed, high quality color laser printers (most offices won’t need these) or slower, good quality ink-jet printers.
- Portable Printers – will you need to print “on the road”? Portable ink-jet printers are reasonably priced.
- Networking: If you plan to network your office, you might want a “network ready” printer or use a print server. Otherwise, you must dedicate a specific computer for network printing (that computer must be turned on for others in the office to print).



Scanners An inexpensive scanner is a good idea for most offices. As we go to a “paperless” office the ability to scan old paper files and then store the file on a CD or floppy disk will prove invaluable.



Telephones The kinds of telephones/phone systems and associated capabilities will be dictated by the level of sophistication of the local phone company in your host country. Some phone companies are quite capable; others aren't. Services you might want to consider are voice mail, call forwarding, call waiting, caller ID, and more. Actual telephone instruments today are offering more and more features; cordless, speaker phone, speed dialing, multiple lines, etc. The key thing is to buy the service and instrument that meets your office needs without needless, excessive, features. Cell phones are becoming an indispensable parts of the modern office; instant communications from anywhere to anywhere. You don't need a cell phone for every member of the SAO; and remember, the office cell phone is for official business.



Projectors Better, smaller, cheaper. They’re still expensive, but if you do a lot of briefings and want to use the computer to show your Power Point briefings then you need one of these.



Fax Machines The most common fax today is the plain paper fax machine. That's all it does - send and receive faxes on plain paper. These are probably the best bet for larger offices that are spread geographically and need multiple fax capability. However, multi-function fax/printers/copiers are starting to make inroads. These might be an attractive, inexpensive, option for a small office of 3-5 people that are co-located



Zip or Jaz Drives You will want to consider either of these if you want to create back-up files for large amounts of data on individual computers or if you're traveling with large files that you don't want to store on a laptop. Zip drives are universally accepted and measured in megabytes (MB) of storage space; 100 MB is a standard size. Jaz drives are measured in gigabytes (GB) of storage space and obviously will cost more than a Zip drive (about twice



as much) because of the additional storage space.

CD ROM and CD Writer Your computers should have a CD-ROM drive. These are becoming standards features of most new computer being purchased today. You might also want to consider a CD writer. The read/write CDs are a great option. You can write large amounts of data to a CD for backups and sharing of programs and files. There are two kinds of CDs on the market today; those that you can write on and then re-write on (like an audio cassette tape), or CDs that can only be written on one time only. *CDs generated with the read/write CDs can only be read by CD ROM drives manufactured starting in 1999!* Another option is one-time write CDs. Although the CDs can't be reused, they are readable in any CD ROM drive. The re-writable CDs are obviously more expensive than the one-time write discs.



Mini Laptops and Palm Pilots These are “neat toys”, but not really necessary for the average USEUCOM SAO. Be prepared to justify their purchase in detail. Remember that these items remain the custody of the SA Office when the individual PCSs.



Digital Cameras If needed, these are no longer cost-prohibitive. In addition, digital cameras making visual record keeping much easier on TDY's where you need a record of sites you've visited; especially if the pictures are part of a trip report or recommendations to the host country and need to be shared with a number of different offices/people. Best results are cameras that use external storage devices (e.g. 3.5 Floppy Disks or PCMCIA (PC Card Reader) Hard Disk). Make sure the zoom function is performed with an optical lens for better quality.



Wiring See Cable, Part V Networking.

Suppressors and Uninterrupted Powers Supplies (UPS) EVERY computer should have a surge suppressor. Critical computers (servers, etc) should have a UPS. UPS for every day use (10 minutes of battery backup) cost less than \$100. Server UPSs that automatically shuts-down the server if your office loses power start about \$500 each. If you're located in a country with commercial power problems (surges, sudden and frequent loss of power, etc) then an UPS is absolutely critical!



Office Automation Equipment Matrix

	1 Person	3 People	10 People
Computer	1	3	10
Printer (B&W)	1	1	2
Printer (Color)			1
CD-ROM		2	8
CD-Writer	1	1	2
Scanner		1	1
External Storage Device (Zip/Jazz)	1	1	3
Laptop	①	1	2
Digital Camera		1	1
Modem ③	1	1	2
Fax	1	1	1
Server		②	1

① May want to consider using docked laptop for a workstation vice a PC.

② One of the PCs can be used as the network server.

③ The number of modems can be reduced with the use of servers.

PART IV: SOFTWARE

Software used on Government computers must be licensed, accredited, and approved by your organization. See your RSO/ISSO for exact requirements. If you want to load private software (e.g. Screen Savers) on your Government computer, you must have a licensed copy and the approval of your supervisor. You may not load any games on your computer.

Operating Systems

Windows 95, Windows 98, or Windows NT? You'll probably want to stay away from Windows NT unless you're planning to run a server based local area network and have the technical administration expertise to run the NT server. Refer to Part V on local area networks and the use of Windows NT.

Don't even consider any other operating system other than those mentioned above! IBM's Warp OS2, Macintosh OS, Linux and Unix are great operating systems, but for a small to medium SAO they're non-starters. USEUCOM won't support them, and there's probably no one in your embassy that can maintain them (in spite of what they might say)!

Office Software

USEUCOM Standards: The current software standards are:

Microsoft Office Professional Suite

MS WORD

MS PowerPoint

MS Access

MS Excel

JetForm FormFlow v 2.x

MacAfee Virus Scan 4.x

The Microsoft Office suite: (Office 97, Office 2000, etc) is the de-facto DoD standard. You might prefer Macintosh (hardware and software), Word Perfect, LOTUS Notes, etc. They're fine on your home PC – but not in the office. Remember the USEUCOM standard! We need to be sure of document compatibility between computers! That great presentation you prepared on your Mac won't impress the general if he can't read it in PowerPoint.

Ensure that you stay with the USEUCOM version standard as well. USEUCOM currently mandates Office 97. Don't upgrade to Office 2000 until directed. Your Office 2000 documents may not be readable by Office 97 at HQ USEUCOM.

Antivirus: It is MANDATORY that anti-virus software be installed and activated on all government computer systems. There are two anti-virus software packages available to all government personnel at no charge (e.g., McAfee and Norton). Both McAfee and Norton Anti-

virus software packages are excellent. They update their virus signatures on a monthly basis and are available on the Internet for download. The software and updates are available at Defense Information Systems Agency's (DISA) web site (<http://199.211.123.12/virus/aviruses.htm>) and the DoD CERT web site (<http://www.assist.mil>). The files on the DISA web site are available to .mil addressees, but the monthly signature files will be in the SAN web library for download.

Compression (WinZip) software: The best \$29 you will spend on your computer. Allows you to quickly and easily compress large files for email transfer.

Photo software: Microsoft offers both Imaging (found under Accessories) and MS Photo Editor in the MS Office Professional package. In addition, most digital cameras come with simple photo-manipulation software.

WEB Browsers: Netscape Communicator & Microsoft Internet Explorer are the market leaders. The Security Assistance community has standardized on Netscape, but most SA web pages work equally well with Internet Explorer.

Calendar Creators and Office Schedulers: Microsoft Outlook (it comes with most versions of Microsoft Office) has powerful built in calendar and scheduling functions that will meet most office needs. A number of simpler (and easier) to use tools are available on the market and might better meet your office needs (simpler is often better than powerful!).

PART V: NETWORKING

Now it's going to get to be fun. There are essentially two setups for a Local Area Networks (LAN) for the small office; peer to peer (all computers equally share the network) and Server based (one computer serves as a "special" machine for file storage, printing, etc.). You can use Windows 95 or Windows 98 to run a peer-to-peer LAN. But you might want to consider adding Windows NT into your office system to run a Server. Windows NT Server has powerful server utilities, but is much more complex to manage. The primary advantage to using Windows NT is that it provides much better security features than either Windows 95 or Windows 98 which are essentially open systems. That's one of the reasons that Windows NT is more complex. HOWEVER, hope is on the horizon. We understand that Windows 2000 will "Plug and Play", which should make installation and maintenance much easier for smaller offices and provide the necessary security.

Client/Server vs. Peer-to-Peer Network.

Client/Server is an architecture in which the client performs the request and the server processes the request and return the result to the client. The server in the Client/Server architecture is also called application server. Compared to peer-to-peer network, Client/Server deploys a dedicated server in the network to fulfill the clients' requests. Therefore, Client/Server means more than having a dedicated server such as a file server.

BENEFITS	DRAWBACKS
Strong central security Central file storage Share available hardware and software Optimized dedicated servers Single password access Easy manageability of large amounts of users Central organization	Expensive dedicated hardware Expensive network operating system software and client licenses A dedicated network administrator

Peer-to-peer network is an architecture in which all the clients in the network can also act as a server. A dedicated file or database server might be used in a peer-to-peer network but it is necessarily required as in a client/server network. This configuration is suitable for networks, which consist of less than 10 computers. Peer-to-peer networks are usually less secure than a server-based network because peer-to-peer networks commonly use share-level security, while server-based networks commonly use file-level or access permission security.

BENEFITS	DRAWBACKS
No extra investment in server hardware or software Easy setup No network administrator required Ability of user of control resources	Additional load on computer because of resource sharing Inability of peers to handle as many network connections as servers Lack of central organization

No reliance on other computers for their operation Lower cost for small networks	No central point of storage for file archiving Requirement that users administer their own computers Weak and intrusive security Lack of central management
---	--

Cable

- **Coaxial Cable** is an inexpensive method of setting up a small network (four computers or less). A hub is not required. Coaxial cable, however, is more difficult to maintain and ANY break in the wire at any place in the network shuts down the entire network.



- **Twisted Pair** Ethernet CAT 5 Cable (i.e., 10 BaseT/100 BaseT). This type of cable is fairly inexpensive and easy to install. A hub is required for network connectivity. Unshielded twisted pair (UTP) is the current defacto standard for most LANs.



- **Fiber Optic Cable** is much more expensive and is much more difficult to install. The advantage of fiber optic is security, speed, and distance. Offices spread out between multiple buildings might want to connect the building networks with Fiber Optic Cable.



- **LAN Cable Specifications** see Appendix 4.

Network Interface Cards (NICs)

- The NIC connects your PC with the network wire.
- You will need NICs for each PC, Laptops, and printers (3-Com is one good choice for less than \$100.00 per card).
- New networks should get the same speed and manufacture of NICs for all PCs if possible.
- Each NIC must have a speed that is compatible with the hub.



Hub

- Used with UTP/STP cables
- A Hub connects the cables from your PC in one central location.
- The hub must support the speed of each NIC connected (typically 10 Mhz or 100Mhz)
- Auto sensing 10/100 hubs are good investments for future growth. They support both older 10 Mhz cards and newer 100Mhz cards.
- A new network should usually have all 100 Mhz NICs and a 100 Mhz hub (it's less expensive the 10/100 hubs).
- Plan on having extra ports for growth (Not too many though because large hubs can get expensive).



- Ethernet switches (they establish “mini networks” between each PC and the server) are fast, but small offices usually won’t benefit from them and they usually cost twice as much as a standard hub.

Server

- A server is generally a good idea for twelve or more computer sharing files or data. The server must have more RAM (128+ MB) and hard drive space (20+ GB) than a typical workstation. It should have a 100 Mhz NIC. You’ll also want a tape drive or other mass-storage backup device.
- Servers can run a variety of operating systems, but we strongly encourage you to use Windows 95/98/NT.
- A Windows 95/98 system can be setup as a server with ease. The only problem using Windows 95/98 systems are security and performance. Windows 95/98 has no more security as a server than as a desktop user PC. Windows 95/98 is not “optimized” for use as a server.
- Setting up a Windows NT Server is a more complicated than Win95/98 but once setup, you’ll have a more secure server. Also, if using NT, you need to have the NT Server software package not the NT workstation software package to run the server.
- Once you have a server in place you will need to:
 - Train your users to save data to the server (where it is more secure).
 - Establish a backup routine on the server to save the data nightly to tape.
- Typical types of servers:
 - File
 - Print
 - Application
 - Message
 - Database



Typical Cyclic Maintenance/Management Requirements

- Create Disaster Recovery Plan
- Back up servers and workstations
- User account management
- Install/remove network software
- Updates to Network Operating System software
- Virus Updates
- Evaluate network usage

Standard Topologies

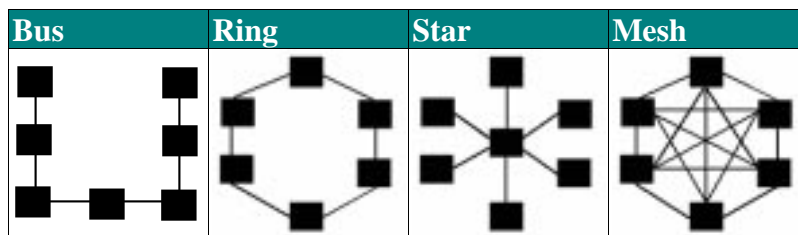
Bus - A single cable (trunk) that connects all computers in a single line.

Star - Computers connect to a centralized hub via cable segments.

Ring - Connects all computers on a single cable. Ends are not terminated like the bus. The cable forms a full loop connecting the last computer to the first computer.

Mesh - Commonly used in wide area network configurations. Routers are connected to multiple links for redundancy and to give the ability to determine the quickest route to a destination.

Topologies Design



Topologies Comparison

BUS	
BENEFITS	DRAWBACKS
Simple, reliable in very small networks, easy to use Least amount of cable Easy to extend Repeater can be used to extend a bus	Heavy network traffic can slow a bus considerably Each connector weakens the signal Difficult to troubleshoot

RING	
BENEFITS	DRAWBACKS
No one computer can monopolize the network Network degrades gracefully as more users are added	Failure of one computer affects the whole network Difficult to troubleshoot Adding or removing computer disrupts the network

STAR	
BENEFITS	DRAWBACKS
Easy to modify and add new computers Center of network is a good place to diagnose network faults Single computer failures do not necessarily bring down the whole network	If the central hub fails, the whole network fails to operate Cable costs are high because of the point to point connections

MESH	
BENEFITS	DRAWBACKS
Major advantage is fault tolerance	Difficult to install and reconfigure
Relatively easy to troubleshoot	Maintaining redundant links

Network Recommendation:

Well all said and done you want to know what is best for you? It is highly recommended, for most SA offices, that a star topology using 10BaseT Ethernet with a peer-to-peer network be installed. This type of network will allow ease of administrations, maintenance, and expandability

PART VI: COMMUNICATIONS AND INTERNET ACCESS

Now that you know what systems you want and how to set them up, how will they communicate with other systems outside of your office? You will need some form of access to the Internet while at home station and/or TDY to access e-mail, the SAN Web, and other critical information on the Web. The following are a few choices.

USG Internet Connection If the embassy already has a high-speed internet connection, usually the fastest, easiest way to connect to the internet is to connect your network into the embassy system.

Dial-up Internet Service Provider (ISP) (AOL, CompuServe, local nation ISPs, etc.): You will need some method of connecting to the Internet. For those offices that don't have direct Internet access via high-speed connection with their LAN (that's most of you), an ISP is a simple and inexpensive way of accessing the Internet.

BENEFITS	DRAWBACKS
Inexpensive (\$500-\$1000 a year).	This is not a continuous connection. Your computer must "dial-out" on a local phone line to establish the connection.
Simple. Usually you get a setup CD that establishes the connection.	Downloads are sometimes slow. You are limited by: the speed of your modem, the quality of local phone lines, and the speed of the ISP modem.
You often can use the same ISP for office Internet and for TDY Internet.	Connections are usually priced per user and per minute. (Try to get a flat rate plan for unlimited use if possible).
Some ISPs offer high-speed (ISDN, DSL, T-1, etc.) dial-up access.	
Better security.	

Direct IDSP Connection The premium Internet connection. You have a continuous connection between your LAN and the Internet.

BENEFITS	DRAWBACKS
FAST! You can get as fast a connection as you are willing to pay for.	Expensive! A few thousand dollars in start-up costs for equipment and thousands of dollars a year for the connection.
Simple day-to-day use. After the LAN is connected to the Internet, every PC on the LAN is connected too!	You'll still need a dial-up ISP connection if you want Internet access while TDY.
If you have an email server, email is immediately available when you turn on your PC (you don't have to manually download).	Security. A network that is available 24 hours a day is available to hackers 24 hours a day.

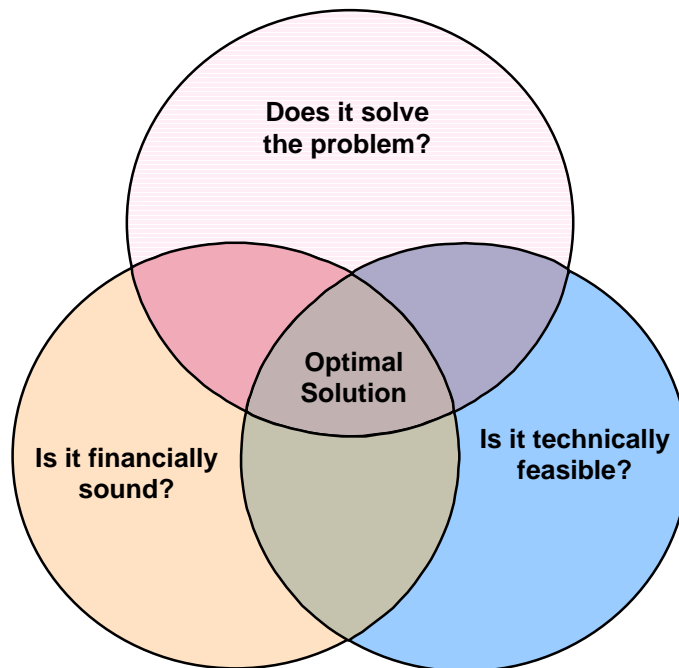
BENEFITS	DRAWBACKS
	Difficult to setup. You'll need an office expert, USEUCOM assistance (if available), and/or local contractor assistance to establish.

PART VII: THE “PRIMARY ROAD MAP”

This road map is simply identification of the fundamental factors that need to be considered in developing an automation plan for any office; regardless of size and costs involved. These factors are shown below. Once you’ve addressed each area you’re ready to develop an automation plan that can be reviewed by outside agencies. If done properly, your plan will withstand any scrutiny.

- Mission Need
- Current Environment
- Desired End State
- Proposed Alternatives
- Cost Analysis
- Service and Maintenance Costs
- Replacement Plan
- Local Unique Requirements and Outside Influences/Demands

Visually, the approach to developing your Automation plan should look like this:



After you've arrived at your "Optimal Solution" you can determine what assets you already have, what you need to obtain from funds within your operating budget and what you might need to submit to HQ USEUCOM as an unfunded requirement (UFR).

PART VIII: REFERENCE LIBRARY

DoD 5200.1R	DoD Information Security Program, Jun 86 (http://web7.whs.osd.mil/dodiss/directives/dir7.html)
DoD 5200.28	AIS Security Program, 21 Mar 88 (http://web7.whs.osd.mil/dodiss/directives/dir7.html)
DoD 5200.40	DoD Information Technology Security Certification And Accreditation Process (DITSCAP), 30 Dec 97
ED 25-1	HQ USEUCOM Information Security SOP, 18 Aug 98 (http://www.eucom.mil/publications/ed/index.htm)
ED 25-5	Information Assurance, 10 Mar 99 (http://www.eucom.mil/publications/ed/index.htm)
ED 90-1	Administration of Security Assistance Organizations/Offices (SAO) (http://www.eucom.mil/publications/ed/index.htm)
SM 100-3	Authorized Use of Government Networks, 5 May 97 (http://www.eucom.mil/publications/sm/index.htm)
SM 100-6	Configuration Management for HQ USEUCOM Standard Automation Information Systems (AIS), 18 Oct 93 (http://www.eucom.mil/publications/sm/index.htm)
SM 100-8	Theater Policy for Defense Information System Network, 26 Mar 99
	Command Inspection Guide for Security Assistance, Section V, 16 Mar 98 (http://www.eucom.mil/hq/ecj4/initiatives/sia_p.htm)
	SAO Inspection Guide, Section IX, 24 May 9

APPENDIX A: ADP Plan Overview

The following is an overview of the five sections that should be including in your plan. This is only an example of how your plan should look, you can be a little creative.

SECTION 1: The approval letter. The Plan must be signed by the SAO/ODC Chief and coordinated with USEUCOM. It is effective for five years, but should be reviewed/updated annually because of the technological advancements in the automation environment. The reason this is a five-year plan is that most ADPE life expectancy is three years.

SECTION 2: The Office Setup/Network Diagram. This section should provide a picture of how the office is setup and answer the who, what, when, and where of automation concerns. Who's working in the ODC? What equipment is used to perform your mission? When was the equipment purchased and when will it need to be replaced? Where is the equipment located? Network Diagram (if applicable). The section provides a snap shot of the ODC's network. It should show what type of network is in place and how the computers systems are connected to it.

SECTION 3: The Hardware Inventory. It should provide future SAO/ODC members and HQ USEUCOM with a clear picture of what hardware is being used. This information will be critical in the ODC's receiving adequate guidance and assistance with the equipment (i.e., repairs, troubleshooting, replacement, etc.).

SECTION 4: The Software Inventory. This section also provides the SAO and HQ USEUCOM with a clear picture of what software is being used. This information will also be critical in USEUCOM or DISAM providing guidance and assistance.

SECTION 5: Projected Requirement Cost. The information in this section will be critical in validating new purchases or replacement items. Granted this information will not be 100 % accurate, but it will be an effective tool in projecting the ADPE funding requirements over a five-year period.

APPENDIX B: ADP Plan Template

ADP PLAN 2000 - 2004
SAO XYZ



(date)
ADP PLAN

Table of Contents

Section 1:	Approval Letter
Section 2:	Office Setup/Network Diagram
Section 3:	Hardware Inventory
Section 4:	Software Inventory
Section 5:	Projected Requirements and Cost

Date

MEMORANDUM FOR HQ USEUCOM J4-ID

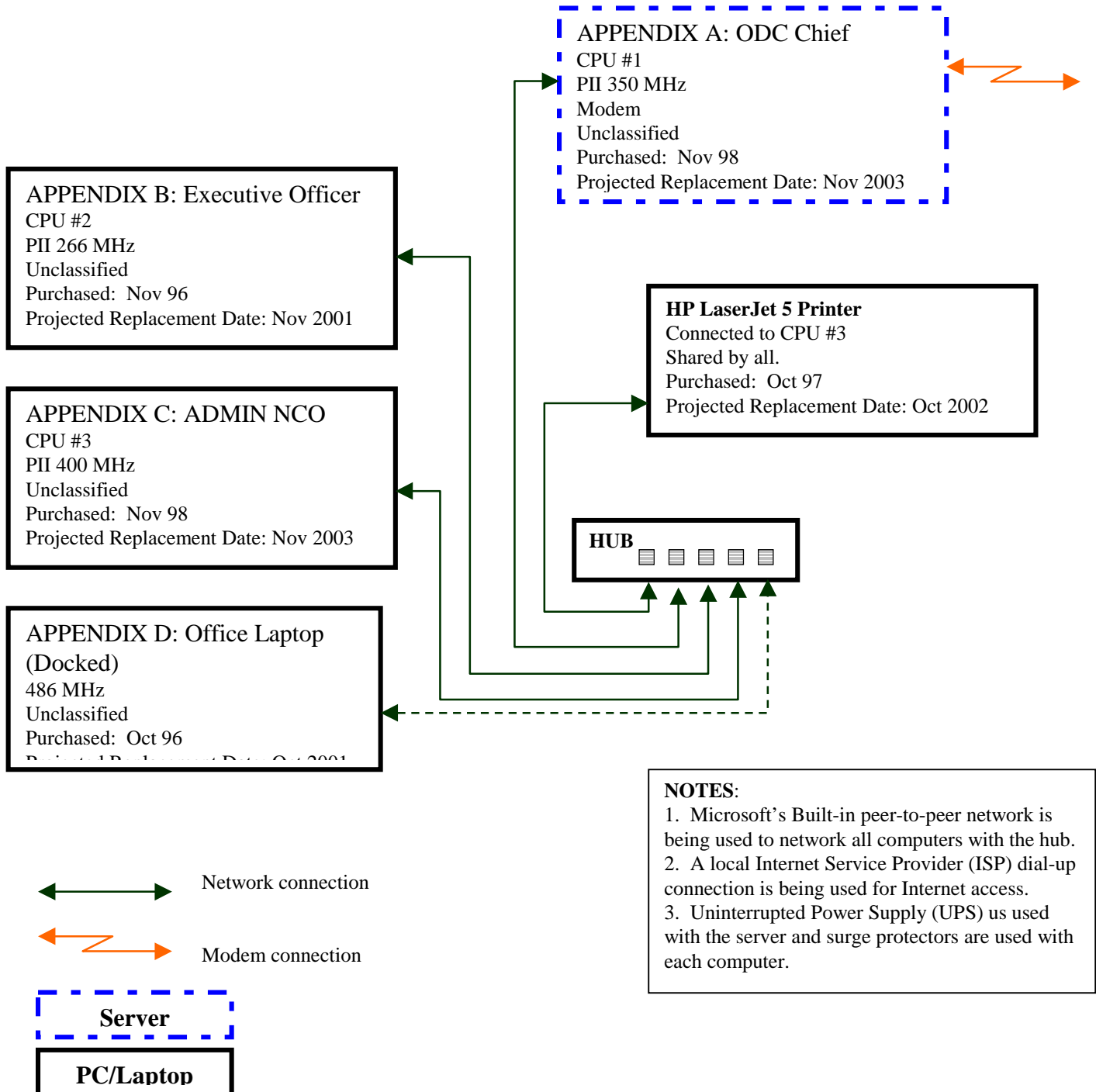
FROM: SAO XYZ

SUBJECT: ADP Plan Approval Letter

I have reviewed the enclosed ADP Plan and grant my approval for its implementation. This plan will be reviewed annually and is effective until 1 January 2004 or until superseded.

SAO Chief XYZ

OFFICE SETUP/NETWORK DIAGRAM (EXAMPLE)



HARDWARE INVENTORY

(Example)

Computer (CPU)								
NUMBER	MAKE	MODEL	SPEED	RAM	DRIVE	MODEM	NIC	CD
1	Gateway	PG1-350	350	64	6.3 GB	33 K	UTP	24 X
2	Gateway	E-3000	266	24	2.3GB	28 K	UTP	4 X
3	Gateway	PG1-400	400	128	6.3 GB	56 K	UTP	32 X

Laptop								
NUMBER	MAKE	MODEL	SPEED	RAM	DRIVE	MODEM	NIC	CD
1	Gateway	Solo	266	64	3 GB	28 K	UTP	12X

Monitor			
MAKE	MODEL	SIZE	CPU #
Gateway	Vivitron	15"	2
Gateway	700	17"	1
Gateway	700	17"	3

Hub		
MAKE	MODEL	PORTS
3COM	Speedy-LAN	12

Printer			
NUMBER	MAKE	MODEL	TYPE
1	HP	4000	B&W

Zip Drives		
MAKE	MODEL	TYPE

Fax	
MAKE	MODEL

Scanner	
MAKE	MODEL

Phones	
MAKE	MODEL

SOFTWARE INVENTORY (Example)

Section 1.01 Operating Systems (OS)	Laptop	CPU 1	CPU 2	CPU 3
(a) Windows 95	X	(i)	X	
Windows 98				X
Windows NT				
UNIX				
Other (specify)				
USEUCOM/DoD Standards				
Word 97	X	X	X	X
Access 97	X	X	X	X
EXCEL 97	X	X	X	X
Power Point 97	X	X	X	X
McAfee 4.0.2	X	X	X	X
Norton 5.0				
Security Assistance Software				
TMS version 4.3	X	X	X	X
SAARMS 1.4	X	X	X	X
a)				
b)				
c) Other Software				
Outlook Express	X	X	X	X
Netscape Communicator	X	X	X	X
Microsoft Internet Explorer (MSIE)	X			
Adobe Acrobat Reader	X	X	X	X
Compression Software (pkzip, pkunzip, etc.)	X	X	(ii)	X
			(iii)	
			(iv)	

Projected Requirements/Cost

FY2000

ITEM	Quantity	COST (each)	Total Cost	Projected Purchase Date	Purchase Type
HUB w/UTP Wires	1	\$500.00	\$500.00	Sep-00	New (Note 1)
Grand Total:					

FY2001

ITEM	Quantity	COST (each)	Total Cost	Projected Purchase Date	Purchase Type
Desktop Computer w/Monitor	1	\$2,500.00	\$2,500.00	Sep-01	Replacement
Laptop	1	\$3,000.00	\$3,000.00	Sep-01	Replacement
Color Printer	1	\$1,500.00	\$1,500.00	Sep-01	New (Note 2)

a. **Grand Total:**
:
\$5500

FY2002

ITEM	Quantity	COST (each)	Total Cost	Projected Purchase Date	Purchase Type
Printer (B&W)	1	\$1,200.00	\$1,200.00	Nov-02	Replacement

b. **Grand Total:**
\$1200.00

FY2003

ITEM	Quantity	COST (each)	Total Cost	Projected Purchase Date	Purchase Type
Desktop Computer w/Monitor	2	\$2,500.00	\$5,000.00	Sep-03	Replacement

c. **Grand Total:**
\$5000.00

d. **Cost Estimates**

CPU/Monitor	\$2,500.00
Printer (B&W)	\$1,200.00
Printer (Color)	\$2,400.00

Laptop	\$3,000.00
Hub	\$400.00
Wiring	\$100.00
Fax	\$400.00
Zip Drive	\$150.00
Office Supplies	\$600.00 Annually

APPENDIX C: LAN Cable Specification

Ethernet Characteristics

TYPE	CABLE TYPES	CONNECTION TYPE	MAX LENGTH
10Base2	Thinnet coaxial cable	BNC T Connector	185 meters (607 ft)
10Base5	Thicknet coaxial cable	DIX/AUI	500 meters (1640 ft)
10BaseT	Category 3, 4, or 5 UTP cable	RJ-45	100 meters (328 ft)
100BaseT	Category 5 UTP cable	RJ-45	100 meters (328 ft)
10BaseFL	Optical Fiber	ST-Single or Multi Mode	2000 meters (615 ft)

Characteristics of Cable

FACTOR	UPT	STP	COAXIAL	FIBER
Cost	Lowest	Moderate	Moderate	High
Installation	Easy	Fairly easy	Fairly easy	Difficult
Bandwidth Capacity	1-to 155Mbps (typically 10Mbps)	1-to 155Mbps (typically 16Mbps)	Typically 10Mbps	2Gbps (typically 100Mbps)
Node Capacity	2	2	30 (10base2) 100 (10base5)	2
Attenuation	High (range of hundreds of meters)	High (range of hundreds of meters)	Lower (range of a few kilometers)	Lowest (range of a few kilometers)
EMI	Most vulnerable	Less vulnerable than UTP	Less vulnerable than UTP	Mot affected

Cost - The cost of each type weighed against the performance and available resources.

Installation - How difficult is it to install.

Bandwidth Capacity - Measures the number of megabits per second (Mbps) that travel through the cable.

Node Capacity - How many computers you can attach easily to the network cables.

Attenuation - Weakening of signal transmitted through the cable over a certain distance.

Electromagnetic Interference - EMI affects the signal sent through the cable.

Categories of Twisted Pair Cable

UTP/STP CATEGORY	SPEEDS
Cat 2	4 Mbps
Cat 3	10 Mbps
Cat 4	16 Mbps
Cat 5	100 Mbps

APPENDIX D: COMPUTER-USER AGREEMENT

As a user of a DoD automated information system, I will adhere to the following security rules:

1. I will use DoD information systems (computers, systems, and networks) only for authorized purposes.
2. I will not import any software or install hardware on any computer (for example, client, workstation, server) without first getting written approval from my systems administrator (SA) or information systems security officer (ISSO), RSO or SAO Chief.
3. I will not try to access data or use operating systems or programs, except as specifically authorized.
4. I know I will be issued a unique identifier and a password to authenticate my identifier (that is, a user ID). After receiving my user ID—
 - a. I will protect the password that authenticates the identifier.
 - b. If I am assigned an individual user account, I will not permit anyone else to use my password, nor will I will I reveal my password to anyone else. If my account is on a classified network, I will protect the password in accordance with the level of the network's classification level.
 - c. I am responsible for all activity that occurs on my individual account once my password has been used to log on.
 - d. I will change my password at once every 3 months.
 - f. I will ensure that my passwords for both classified and unclassified accounts meet current DoD standards (for example, length, character set, no prohibited sequences or combinations) as directed by the ISSO/RSO.
 - g. I will not store my password on any processor or microcomputer or on any magnetic or electronic media unless approved in writing by the ISSO/RSO.
 - h. I will not tamper with my computer to avoid adhering to DoD password policy.
 - i. I will never leave my classified computer unattended while I am logged on or unprotected by a password-protected screensaver.
5. I know that it is a violation of policy for any computer user to try to mask or hide his or her identity, or to try to assume the identity of someone else.
6. I know that if connected to the Secure Local Area Network (SLAN), my system operates at least in the U.S. Secret, "system-high" mode.

- a. Any magnetic media used on the system must be immediately classified and protected at the system-high level, regardless of the implied classification of the data (until declassified or downgraded by an approved process).
 - b. I must protect all material printed out from the SLAN at the system-high level until someone, or I with the appropriate clearance personally reviews and classifies the material.
 - c. I will not enter information into a system if the information has a higher classification than the system. I will not enter information that is proprietary, contractor-excluded, or otherwise needs special protection or handling, unless approved in writing by the ISSO/RSO.
 - d. If connected to the SLAN, only U.S.-cleared personnel are allowed unescorted access to the system.
 - e. Magnetic disks or diskettes will not be removed from the computer area without the approval of the local commander or head of the organization.
7. I will check all magnetic media for malicious software before loading it onto a DoD system or network.
8. I will not forward chain mail or virus warnings. I will report chain e-mail or virus warnings to my ISSO/RSO and delete the message. I will not attempt to run "sniffer" or other hacker-related software on the system.
9. I know I am subject to disciplinary action for any violation or abuse of access privileges.
10. If I observe anything that indicates inadequate security on the system I am using, I will immediately notify the site ISSO/RSO. I know what constitutes a security incident and know that I must immediately report such incidents to the ISSO/RSO.
11. I will comply with security guidance issued by my systems administrator, ISSO and RSO.
12. I understand that this agreement merely summarizes key points governing the use of Government computers in DoD, and is not an all-inclusive list of requirements and procedures governing the use of DoD computers.

I understand this agreement and will keep the system secure. If I am the SAO Chief, systems administrator, or ISSO, I will ensure that all users in my area of responsibility sign this agreement.

Name: _____

Signature: _____

Date signed: _____

7. Keep personal files stored on network drives and local hard drives to a minimum.
8. Use Anti-Virus Software to scan downloaded files, e-mail attachments, and floppy disks before opening them.
9. Your use of government systems must not incur any tolls, charges or other fees, except when specifically authorized **in writing**.
10. Your use must not solicit business, advertise, or engage in any other selling activities in support of private business.

Information is from Staff Memorandum Number 100-3

HQ USEUCOM SLAN REMOTE USERS

SLAN USERID's are **UNCLASSIFIED!**
SLAN PASSWORDS are **SECRET!!!**

Do not give anyone the telephone numbers for remote dial-up access to the SLAN.

Do not move your SLAN workstation or STU-III to a new location and remotely access the SLAN.

Do not access the SLAN by other than approved remote access means.

The **SLAN** is authorized to process classified data up to and including U.S. SECRET.

The **SLAN** is **NOT authorized** to process: TOP SECRET, SCI, ORCON, NATO classified data, SIOP-ESI, CNWDI, SPECAT, or contractor proprietary information.

Classified or formerly classified computer storage media shall be declassified and/or destroyed in accordance with the HQ USEUCOM Computer Networks Security Features User's Guide (SFUG).

The **SLAN** may be used to coordinate PERSONAL FOR messages prior to official release. The Secretary Joint Staff (SJS) controls access to incoming PERSONAL FOR messages.

Use of the **SLAN** is for **official use only** as defined by USEUCOM Staff Memorandum on Automation Matters (SM 100-3).

LABELING AND RELEASE OF OUTPUT DATA FOR REMOTE SLAN USERS

Remember: Your computer cannot automatically identify data by security classification, SO

-Protect all hard copy output as SECRET until someone who is knowledgeable of the data reviews it in its entirety and determines the security protection required!

-Clearly label all removable media which has been used for any reason in an SLAN system as SECRET.

-If you create classified e-mail, label the subject line and text with security markings as described in the SLAN User Guide.

-Clearly label all SLAN equipment that can store or display data as SECRET.

POINTS OF CONTACTS

ECJ4-ID Automation and Training

Ms Mairi Marquart
Marquart@eucom.mil
DSN: 430-7479
Com: 49-711-680747

TSgt Donald Lewis
lewisd@eucom.mil
DSN: 430-7456
Com: 49-711-6807456



ECJ6-I Information Assurance

ISSM LT Nina Kenmore
Kenmoren@eucom.mil
DSN: 430- 5341
Com: 49-711-680 5341

C4I HelpDesk (SLAN Remote Users)

Helpdesk@eucom.smil.mil
DSN: 430-4174
Com: 49-711-6804717



TOP TEN SECURITY MEASURES

1. Back up your files.
2. Pick proper passwords.
3. NEVER divulge your password!
4. Use Anti-Virus software.
5. Don't violate software copyright law.
6. Use a surge protector.
7. Keep food and drinks away from your computer.
8. Use a screen saver with a password.
9. Place your computer on a sturdy table.
10. Do NOT move network computer equipment yourself, contact your systems administrator for assistance.

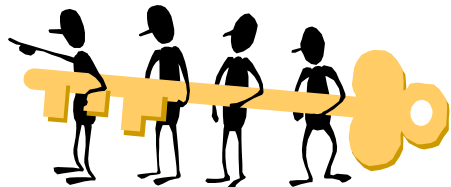


USERID's and PASSWORDS

Userid and password are required for access to all officer computer systems.

Each user is personally responsible for protecting and properly using their userid and password.

USERID's and passwords are individual identifiers, so:
-do NOT use any means other than your USERID and password to access the PC,
-do NOT divulge your password to any other person,
-and NEVER forget to log off when you leave your workstation!



GENERAL RULES AND PROCEDURES

The Office PC is authorized to process unclassified data only to include For Official Use Only (FOUO) and Sensitive But Unclassified (SBU) information.

It is **NOT authorized to process any classified** information such as CONFIDENTIAL, SECRET, TOP SECRET, SCI, ORCON, NATO classified data, etc. Use of the office PC is for **official use and authorized purposes only** as defined by SM 100-3.

Use of any DOD-interest computer system constitutes consent to being monitored at all times.

Users shall **NOT**:

- a. Relocate equipment out of its approved operating area,
- b. Add to equipment, or
- c. Copy proprietary or personal software on to a government computer system.

Users shall report to the unit Security Manager any violation of security procedures or other security problems encountered while using office PCs

Requests for any variations from the provisions of this pamphlet shall be sent to the \your security manager or ECJ4-ID.

QUESTIONS?

**Contact your local Security Manager or
ECJ4-ID 49-711-6807479**

COMPUTER VIRUSES

All computer storage media, regardless of its origin, must be scanned for viruses prior to use.

If a virus is detected: (1) discontinue operations with the infected system, (2) notify your security manager or ECJ4-ID, (3) collect and secure all removable media

that may have been used recently in the infected system, and (4) await further instructions from your security manager or ECJ4-ID.

AUTHORIZED USE OF GOVERNMENT COMPUTER NETWORKS

AUTHORIZED USES

1. You MAY use network resources, such as e-mail, mailing lists, news groups, and the WWW for professional development and continuing education purposes, if it does not impede your primary duties and mission.
2. You MAY use network resources for other personal reasons, such as occasional e-mail to spouse or minor children, scheduling appointments, brief internet searches, and reading professional magazines.
3. You MAY use e-mail and other network resources in support of your personal and private participation in non-Federal, not-for-profit professional organizations or learned societies. Make sure you get prior approval from your supervisor!

RESTRICTIONS

1. Your use must not adversely affect or impede the performance of official duties.
2. Your use must serve a legitimate public interest, such as keeping you at your work place, enhancing skills, furthering education, or improving morale.
3. Your use must be during your off-duty hours or during authorized breaks.
4. Your use must not overburden the network.
5. Your use must not result in significant use of consumable resources (i.e., printer paper and toner).
6. Abide by applicable licensing agreements and software copyrights. All non-supported software must be legally purchased and approved by your agency, office, or directorate. **No personal software of any kind shall be approved for installation on government computers.**